UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

RANDOLPH FRESHOUR and VINCENZO ALLAN, each individually and on behalf of similarly situated individuals,	)	No. 1:23-cv-02667
Plaintiffs,	)	Hon. Nancy L. Maldonado
v.	)	Magistrate Judge M. David Weisman
CERENCE INC., a Delaware corporation,	)	
Defendant.	)	

THIRD AMENDED CLASS ACTION COMPLAINT[1]

Plaintiffs, Randolph Freshour and Vincenzo Allan, each individually and on behalf of other similarly situated individuals, bring this Third Amended Class Action Complaint against Defendant, Cerence Inc. ("Cerence"), to stop Defendant from violating the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.* and to seek redress for those aggrieved by Defendant's unlawful conduct. Plaintiffs allege as follows based on personal knowledge as to their own acts and experiences, and as to all other matters, on information and belief, including an investigation by their attorneys.

NATURE OF THE ACTION

1. Defendant Cerence is a multinational software and technology company that provides voice and speech recognition technology for automobiles. Defendant's products use

[1] The Court's June 1, 2023 Order (Dkt. 16) severed and remanded Counts I and III of the original Class Action Complaint filed in this litigation (Dkt. 4-1) due to lack of federal subject matter jurisdiction. The claims pled under those counts have been realleged in an amended pleading filed in the state court companion case to this matter. Plaintiffs do not waive or forfeit, and hereby expressly preserve, all rights with respect to those claims.

biometric-enabled systems to listen to drivers and passengers voices, deliver personalized responses, and perform tasks related to navigation, entertainment, and climate control. Many of the automobiles embedded with Defendant's software "listen[ ] to almost every word and understand[ ] practically any sentence relating to infotainment sector and vehicle operation[.]"[2]

2. In order to process users' voice commands and perform tasks specific to an individual speaker, Defendant's software captures, stores, and processes users' voiceprints—the unique characteristics of their voice—for identification and verification purposes. With a voiceprint, Defendant's software can identify an individual based on the unique features of their voice for the purpose of carrying out personalized tasks such as playing the speaker's favorite music or completing online purchases. Defendant's software can even remember past interactions with a particular individual and reactivate preset settings, such as certain seat positions.

3. Voice recognition technology—which utilizes individuals' biologically unique voiceprints—is subject to the Illinois Biometric Information Privacy Act, or BIPA. BIPA protects individuals' biometric privacy rights by regulating private entities' collection and use of biometrics. For instance, BIPA prohibits a private entity from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric data or biometric information (collectively, "biometrics") unless it: (1) informs that person in writing that biometric identifiers and information will be collected and/or stored, (2) informs the person in writing of the specific purpose and length for which the biometric identifiers or information are being collected, stored, or used, (3) receives a written release from the subject, and (4) publishes publicly available written retention schedules and guidelines for permanently destroying said biometrics. *See generally* 740

[2] Meet the S-Class DIGITAL: "My MBUX" (Mercedes-Benz User Experience), available at https://media.mbusa.com/releases/release-9e110a76b364c518148b9c1ade19bc23-meet-the-s-class-digital-my-mbux-mercedes-benz-user-experience (last accessed 7/13/2023).

ILCS 14/15(a), (b).

4. When Defendant provided its biometric-enabled technology for integration with automobiles sold and driven in Illinois, its actions triggered a number of statutory requirements under BIPA. However, Defendant has failed to meet its legal obligations under BIPA. For instance, Defendant never published a compliant retention policy and destruction guidelines for Plaintiffs' and the other putative class members' biometrics; it never provided the required disclosures about the specific purpose and length of time for which Plaintiffs' or the other putative class members' biometrics would be stored or used; and Defendant never sought a signed, written release from Plaintiffs or the other putative class members prior to obtaining their biometrics.

5. Accordingly, Plaintiffs bring this action for statutory damages and other available relief as a result of Defendant's unlawful conduct and its violations of Plaintiffs' biometric privacy rights under BIPA. Individually and on behalf of a proposed class defined below, Plaintiffs seek declaratory and injunctive relief as well as an award of statutory damages, litigation costs, reasonable attorneys' fees, and prejudgment interest.

PARTIES

6. At all relevant times, Plaintiff A.P. and her guardian, Plaintiff Carlos Pena, have both been residents of Illinois.

7. At all relevant times, Plaintiff Randolph Freshour has been a resident of Illinois.

8. At all relevant times, Plaintiff Vincenzo Allan has been a resident of Illinois.

9. Defendant Cerence Inc. is a for-profit corporation organized under the laws of Delaware and headquartered in Burlington, Massachusetts.

JURISDICTION AND VENUE

10. Defendant removed this case pursuant to the Class Action Fairness Act, 28 U.S.C.

§ 1332(d) *et seq.*, asserting that: the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are greater than 100 putative class members; at least one putative class member is a citizen of a state other than Defendant; and none of the exceptions under subsection § 1332(d) apply.

11. This Court has personal jurisdiction over Defendant with respect to Plaintiffs' and the putative class members' claims, because Defendant knowingly and intentionally transacts business within Illinois such that it has sufficient minimum contacts with Illinois and has purposely availed itself of Illinois markets to make it reasonable for this Court to exercise jurisdiction over Defendant, and because Plaintiffs' and the putative class members' claims arise out of or relate to Defendant's unlawful in-state conduct, as Defendant's violations of BIPA occurred within this Illinois.

12. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant resides in this District under § 1391(c)(2), and because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District.

ALLEGATIONS OF FACT COMMON TO ALL COUNTS

The Biometric Information Privacy Act

13. "Biometrics" refers to a "biology-based set[s] of measurements." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, "biometrics" are "a set of measurements of a specified physical component (eye, finger, voice, hand, face)." *Id.* at 1296.

14. BIPA was enacted in 2008 in order to safeguard individuals' biometrics as a result of the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276.

15. As set forth in BIPA, biologically unique identifiers, such as a person's unique

fingerprints, voiceprint, or facial geometry, implicate special concerns because they cannot be changed:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

740 ILCS 14/5(c).

16. As the Illinois Supreme Court has held, BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court further held that when a private entity fails to comply with BIPA, "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." *Id.*

17. Due to the critical need for enhanced protection of biometrics, BIPA imposes various requirements on private entities with respect to individuals' biometrics.

18. Among other things, BIPA regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). BIPA thus applies to entities that interact with two forms of biometrics: biometric "identifiers" and biometric "information." 740 ILCS 14/15(a)–(e).

19. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including fingerprints, voiceprints, palm scans and facial geometry. "Biometric identifiers" are physiological, as opposed to behavioral, characteristics. BIPA's text provides a non-exclusive list of protected "biometric identifiers," including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

20. "Biometric information" is defined by BIPA as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id*. This definition helps ensure that information based on a biometric identifier that can be used to identify a person is covered by BIPA. Collectively, biometric identifiers and biometric information are known as "biometrics."

21. In Section 15 of BIPA, there is a list of at least four distinct categories of activities that may subject private entities to liability:

a. possessing biometrics without making publicly available a written biometric retention and destruction policy, 740 ILCS 14/15(a);

b. collecting biometrics without informed written consent, 740 ILCS 14/15(b);

c. profiting from biometrics, 740 ILCS 14/15(c); and

d. disclosing or disseminating biometrics without consent, 740 ILCS 14/15(d).

22. Compliance with BIPA is straightforward for those who wish to use biometric technology, and generally may be accomplished through a single, signed sheet of paper.

Defendant's Use of Biometric-Enabled Technology

23. Defendant Cerence Inc. is a multinational technology company and a provider of AI voice assistant and voice recognition technology for automobiles. Specifically, Defendant is the provider of the Cerence Drive platform, which includes products and services that Defendant sells to its automotive manufacturer customers for integration in consumer automobiles.

24. Defendant's products and services are integrated with more than 450 million automobiles' in-car systems, including automobiles manufactured and sold to consumers by

Volkswagen, Mercedes-Benz, Toyota, Honda, Subaru, and many others.

25. Automobiles integrated with Cerence Drive typically incorporate a host of Cerence software and other technology, including a biometrically-enabled voice assistant, microphones placed throughout the vehicle's interior, and voice recognition software installed on the vehicle's operating system.

26. Cerence Drive's voice recognition technology is capable of not only receiving, understanding, and carrying out voice commands, but also identifying the person who made a particular voice command and where they are, so that the system can tailor its responses or actions to that specific person. In other words, Cerence Drive's technology can determine the identity of a person delivering commands and also where he or she is seated in the cabin.

27. Cerence Drive performs the capabilities mentioned above by collecting, processing, analyzing, and storing users' voiceprint biometrics. On Defendant's website, a screenshot of which is depicted in Figure 1 below, Defendant provides a description of its use of voice biometrics.[3]

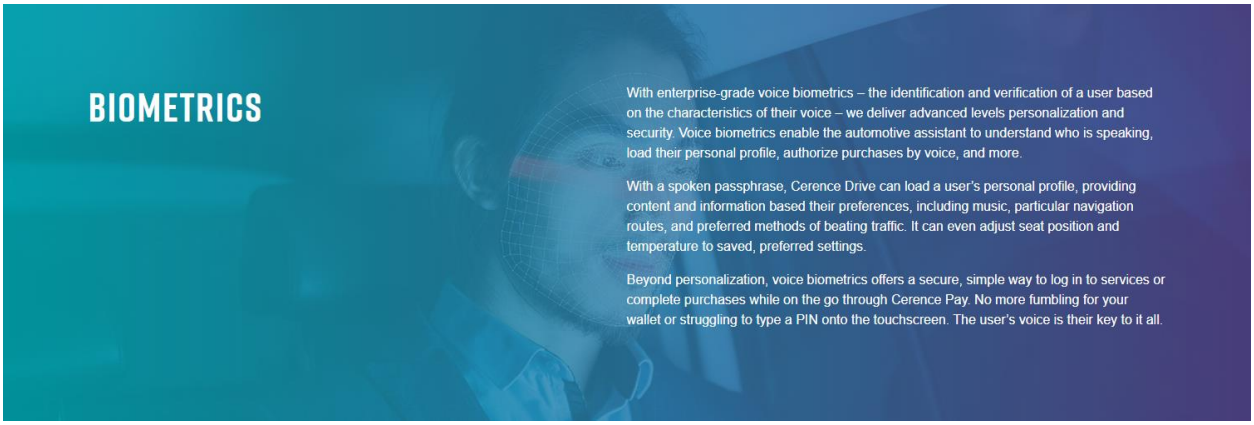

Figure 1.

28. As shown in Figure 1, Cerence uses "voice biometrics – the identification and verification of a user based on the characteristics of their voice" to "deliver advanced levels of

[3] https://www.cerence.com/cerence-products/beyond-voice (last accessed 3/24/23).

personalization" and "enable the automotive assistant to understand who is speaking, load their personal profile, authorize purchases by voice, and more."

29. Indeed, in a September 2, 2020 press release from Cerence, Cerence states that many automobiles embedded with Cerence technology utilize "Biometric Identification & Personalization" to "identify who is speaking based on a memory of known speakers," which enables the software to "activate a personalized profile that stores information about that speaker, such as favorite radio stations, personal navigation destinations, and the mirror and seat settings."[4] Cerence Drive technology is capable of distinguishing a user who has a personalized profile from other speakers based on the voiceprint associated with the user profile.

30. Importantly, Cerence itself collects, captures, and stores the unique voiceprint biometrics of individuals who interact with Cerence's voice assistant technology. Cerence confirms on its website that "[w]hen you use Cerence voice recognition technology, whether by using Cerence's own Products or by using third party products that employ Cerence voice recognition technology, we may capture your voice and the words that you speak into the product."

31. Cerence Drive technology also uses "Speech Signal Enhancement," or SSE, to detect and isolate certain voices and filter out others, so that Cerence Drive's voice assistant software can determine who may be making a voice command, and who else in the automobile should be muted or ignored. SSE is a core functionality of Cerence Drive.

32. Figure 2, below, shows a screenshot from Cerence's 2020 Technology Showcase where Udo Haiber, Vice President of Research and Development at Cerence, explained how Cerence's SSE can identify and isolate the voice of a speaker through its Deep Neutral Network

[4] Our Four Favorite Features in the Next-Gen MBUX, https://www.cerence.com/news-releases/news-release-details/our-four-favorite-features-next-gen-mbux (last accessed 7/13/2023).

(DNN) Noise Cancelation System.[5]

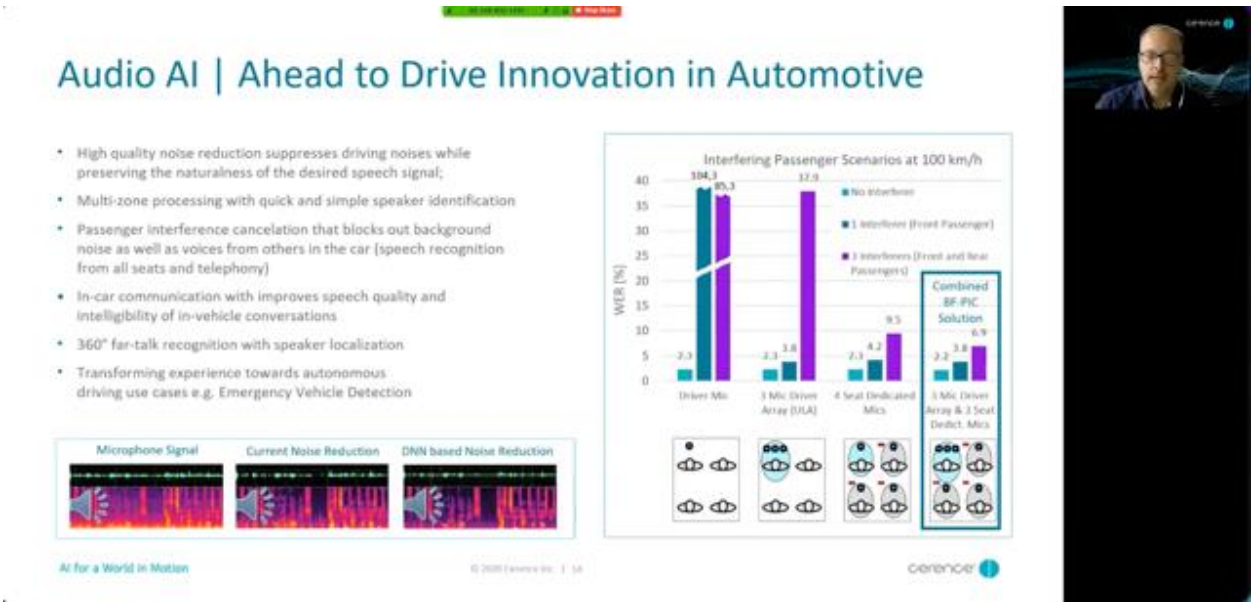

Figure 2.

33. Notably, the slide depicted in Figure 2 contains spectrograms of voices. A spectrogram is a visual graph used to display frequencies of sound waves. For illustrative purposes, Figure 3 below depicts an example of a spectrogram of a human voice.

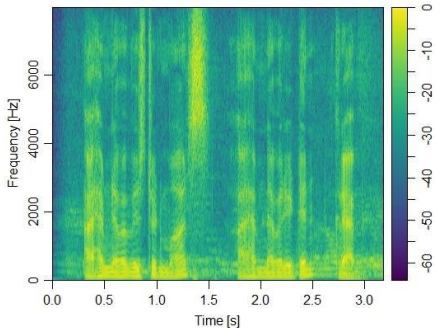

Figure 3.

34. A spectrogram of a human voice, like the kinds depicted in Figures 2 and 3, is derived from biometric identifiers and is a type of biometric information, and can be used to

[5] Cerence Technology Showcase, available at https://www.youtube.com/watch?v=uBcZ1aoL16s at 46:00 – 48:00 (last accessed 7/13/2023).

identify an individual by the unique attributes of the sound of his or her voice.

35. The spectrograms in Figure 2, which depict voices detected and analyzed by Cerence Drive, further demonstrate how Cerence Drive uses SSE to collect voiceprints and/or other biometric information derived therefrom and isolate the voiceprint from other ambient noise.

36. Once Cerence obtains users' biometric identifiers, biometric information, and/or data derived therefrom, Cerence's software sends that data and information to and from its servers and servers hosted at datacenters belonging to third parties.[6] Cerence "use[s] multiple data centers and cloud hosting to provide the compute power for [its] products," and Cerence's "product systems are designed to seamlessly shift data and compute resources between the cloud and computer systems that are onboard vehicles[.]"[7] These servers aid Cerence's voice assistant technology and software in supplying responses to user queries or performing tasks.[8]

37. In addition to collecting and storing voice biometric data, Cerence also processes and analyzes that data for multiple purposes, including to help Cerence's software determine whether a user has made or attempted to make a voice command, whether the speaker is someone who has a registered profile, and whether the speaker is someone that Cerence's software recognizes from a prior interaction.

38. Cerence also utilizes biometric information and other data derived from biometrics to create usage statistics and improve its services. Cerence's biometric-enabled technology "is

[6] Cerence-powered technology includes "[i]ntegration of embedded and cloud speech for quick and accurate interaction with the assistant, even in areas of low connectivity." Cerence Voice Powers Voice and AI-Driven Features in Next-Generation Mercedes-Benz User Experience (MBUX), available at https://cerence.com/news-releases/news-release-details/cerence-powers-voice-and-ai-driven-features-next-generation (last accessed 7/13/2023).

[7] Cerence 2021 Environmental, Social and Governance Report, available at https://sustainserv.com/wp-content/uploads/2021/11/Cerence-ESG-Report-2021.pdf.

[8] "Both the head unit in the vehicle and the server evaluate the data and send a reply." *See supra* note 2.

constantly learning driver preferences based on previous commands and behaviuors [sic], making interaction with the assistant increasingly intuitive over time."[9]

39. Moreover, Cerence disseminates biometric data it collects to third-parties and data storage vendors. Cerence splits the data it collects "between onsite server rooms and two third-party data centers," and information that Cerence "customers use is hosted in third-party public clouds that [Cerence] directly manage[s]." *Id.*

40. Cerence's in-car technology interfaces with and has access to many external content services that it utilizes to respond to voice commands. For example, Cerence Drive can use voice commands to log into third-party services to find destinations, provide navigation routes, make purchases, and play music through music streaming applications.

41. Since at least as early as 2019, Defendant has partnered with numerous automobile manufacturers to integrate Cerence Drive voice assistant technology and SSE capability into the operating systems of some of the most popular consumer automobiles. For example, Mercedes-Benz models that are equipped with the second generation Mercedes-Benz User Experience, or "MBUX" system, are powered by Cerence's biometric-enabled voice assistant technology. As stated in a December 15, 2020 press release, the "second generation of MBUX" offers "enhanced personalization and security leveraging a variety of biometric technologies, including voice biometrics from Cerence. This enables quick access to personalized settings, from navigation and multimedia preferences to seat position and the perfect temperature, all with identification by voice."[10]

42. Although Cerence's voice recognition technology is a core part of the AI voice

[9] VW Selects Cerence to Power Conversational AI in its Next-Gen Infotainment System, available at https://archive.autofutures.tv/2022/03/02/vw-selects-cerenc/ (last accessed 7/13/2023).
[10] *See supra* note 6.

assistant systems present in many automobiles, Cerence does not clearly inform or notify the drivers and passengers of those vehicles that it is collecting, capturing, storing, and disseminating their voiceprint biometrics. Additionally, Cerence fails to obtain written consent from end-users to collect, possess, store, use, or disseminate their voiceprint biometrics.

43. Defendant has also unlawfully profited from the voiceprint biometrics that it obtained from Plaintiffs and other individuals in Illinois. Defendant charges its automobile manufacturer customers for its Cerence Drive voice assistant technology and services. By selling and licensing its AI voice assistant hardware, software, and services to automotive manufacturers, Cerence directly profits from users' biometrics.[11] Additionally, collection of biometrics is an essential element of Defendant's business model. The collection, storage, and dissemination of users' biometrics is core to the functionality of Cerence Drive, so Cerence's business is reliant on the collection of voiceprint biometrics from end users.

44. On information and belief, Cerence also collects and stores location data and other personally identifiable information when users engage with its platform. Accordingly, Defendant knows that its technology will and has interacted with individuals located in the state of Illinois, such as Plaintiffs, without regard for compliance with BIPA's requirements.

Facts Specific to Plaintiff Randolph Freshour

45. As stated above, Defendant's biometric-enabled voice recognition technology and SSE capability are integrated into the second generation MBUX systems in many newer consumer automobiles manufactured and sold by Mercedes-Benz.

[11] Cerence "generate[s] revenue primarily by selling software licenses and cloud-connected services, and secondarily from our professional services to OEMs and their suppliers during vehicle design, development and deployment." Cerence 2021 Environmental, Social and Governance Report, available at https://sustainserv.com/wp-content/uploads/2021/11/Cerence-ESG-Report-2021.pdf.

46. The Cerence-powered MBUX system utilizes voice biometrics "to recognise vehicle occupants by their voices," and "[o]nce the individual characteristics of the voice have been learned, this can be used to access personal data and functions by activating a profile."[12] For example, MBUX uses "[b]iometric authentication by fingerprint, face or voice" for security purposes, as well as voice biometrics for tasks like "accepting a telephone call or displaying the navigation map."[13]

47. In or about August of 2022, Plaintiff Randolph Freshour purchased a 2021 AMG GLC43 model Mercedes-Benz. Upon arriving to his home in Illinois, Plaintiff Freshour's automobile's operating system prompted him to make a personal profile with the "MBUX" voice assistant system powered by Cerence Drive.

48. As part of the process for creating the user profile, Plaintiff Freshour was required to provide his first and last name and email address.

49. During the registration process, Plaintiff Freshour was also prompted to repeatedly say "Hey Mercedes" to the MBUX voice assistant so that the software could collect his voiceprint in order to learn and recognize his voice. Unbeknownst to Plaintiff, however, Defendant's Cerence Drive software was integrated into the MBUX voice assistant and was collecting, capturing, obtaining, and storing Plaintiff Freshour's voiceprint and relating his biometric voiceprint data with his profile.

50. Following registration with the MBUX voice assistant, every instance in which Plaintiff Freshour said "Hey Mercedes" in his vehicle to carry out tasks and adjust settings such as those related to navigation, music selection, and cabin temperature, Defendant's biometrically-

[12] MBUX reaches a new level, available at https://group.mercedes-benz.com/innovation/digitalisation/connectivity/mbux-interior-assist.html (last accessed 7/13/2023).
[13] *See supra* note 2.

enabled voice assistant software which powers the MBUX voice assistant would collect, capture, and store Plaintiff Freshour's voiceprint. Defendant's software did this both for identify verification purposes—to confirm that the speaker's voiceprint matched the one stored previously—and to activate and display Plaintiff's profile and load his personal settings.

51. Despite collecting, capturing, obtaining, and disseminating Plaintiff Freshour's voiceprint biometrics, Defendant failed to obtain valid written consent as required by BIPA. Defendant also failed to provide Plaintiff Freshour with any written disclosures informing him of the specific purpose and length of term for which his biometrics were being collected.

52. Further, on information and belief, Defendant unlawfully disclosed Plaintiff Freshour's and other Class members' biometrics to its third-party cloud and data storage vendors without Plaintiff's informed consent.

Facts Specific to Plaintiff Vincenzo Allan

53. During the time period relevant to this action, Plaintiff Vincenzo Allan has owned several Mercedes-Benz automobiles integrated with MBUX and voice assistant technology powered by Cerence's voice recognition and SSE capability, including a 2020 Mercedes-Benz AMG C 63 S purchased in or about November of 2019, a 2022 Mercedes-Benz S580 purchased in or about March of 2022, and a 2023 Mercedes-Benz E 63 S purchased in or about May of 2023.

54. After each of the above-mentioned purchases, Plaintiff Allan returned to his home in Illinois and was prompted by the automobile's operating system to make a personal profile with the MBUX voice assistant system powered by Cerence Drive.

55. As part of the process for creating the user profile, Plaintiff Allan was required to provide his first and last name and email address.

56. During the registration process for each vehicle, Plaintiff Allan was also prompted

to repeatedly say "Hey Mercedes" to the MBUX voice assistant so that the software could collect his voiceprint in order to learn and recognize his voice. Unbeknownst to Plaintiff, however, Defendant's Cerence Drive software was integrated into the MBUX voice assistant and was collecting, capturing, obtaining, and storing Plaintiff Allan's voiceprint and relating his biometric voiceprint data with his profile.

57. Following registration with the MBUX voice assistant, every instance in which Plaintiff Allan said "Hey Mercedes" in one of his vehicles to carry out tasks and adjust settings such as those related to navigation, music selection, and cabin temperature, Defendant's biometrically-enabled voice assistant software which powers the MBUX voice assistant would collect, capture, and store Plaintiff Allan's voiceprint. Defendant's software did this both for identify verification purposes—to confirm that the speaker's voiceprint matched the one stored previously—and to activate and display Plaintiff's profile and load his personal settings.

58. Despite collecting, capturing, obtaining, and disseminating Plaintiff Allan's voiceprint biometrics, Defendant failed to obtain valid written consent as required by BIPA. Defendant also failed to provide Plaintiff Allan with written disclosures informing him of the specific purpose and length of term for which his biometrics were being collected.

59. Further, on information and belief, Defendant unlawfully disclosed Plaintiff Allan's and other Class members' biometrics to its third-party cloud and data storage vendors without Plaintiff's informed consent.

CLASS ALLEGATIONS

60. Plaintiffs bring this action individually and, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as representatives on behalf of a Class defined as follows:

> All persons who: (1) owned, leased, and/or created a user profile for an automobile with Cerence Drive-powered voice recognition technology;

> (2) whose voiceprint biometric identifiers or biometric information were collected, captured, used, stored, disseminated, transmitted, possessed and/or otherwise obtained by Defendant; (3) while the automobile was within the state of Illinois; (4) at any time between five years prior to the filing of this action through the present.

61. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officers, directors, or employees of Defendant; and any immediate family members of such officers, directors, or employees.

62. On information and belief, there are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiffs, the members can be easily identified through Defendant's records and Defendant's customers' records.

63. Plaintiffs' claims are typical of the claims of the Class members they seek to represent, because the basis of Defendant's liability to Plaintiffs and the Class members is substantially the same, and because Defendant's conduct has resulted in similar harms to Plaintiffs and to the Class. As alleged herein, Plaintiffs and the Class have all been aggrieved as a result of Defendant's BIPA violations.

64. There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant's Cerence Drive voice recognition technology collects, captures, or otherwise obtains biometric identifiers or biometric information from Illinois users;

b. Whether Defendant's conduct is subject to BIPA;

c. Whether Defendant made available to the public a written

policy that establishes a retention schedule and guidelines for destroying biometrics;

d. Whether Defendant obtained a written release from the Class before capturing, collecting, or otherwise obtaining their biometrics;

e. Whether Defendant provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored and used, before taking such biometrics;

f. Whether Defendant disseminated or disclosed the Class members' biometrics to third parties without the subjects' consent;

g. Whether Defendant's profiting from the collection of Class members' biometrics violates BIPA;

h. Whether Defendant's conduct violates BIPA;

i. Whether Defendant's violations of the BIPA are willful or reckless; and

j. Whether Plaintiffs and the Class are entitled to damages and injunctive relief.

65. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes

consistency and efficiency of adjudication.

66. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class they seek to represent. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

67. Defendant has acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b)
(On behalf of Plaintiffs and the Class)

68. Plaintiffs incorporate the foregoing allegations by reference as though fully set forth herein.

69. Defendant is a private entity subject to BIPA. 740 ILCS 14/10.

70. As discussed above, Plaintiffs and the other Class members have had their "biometric identifiers," namely their voiceprints and/or data derived therefrom, *i.e.*, "biometric information," collected, captured, and obtained by Defendant when they interacted with Defendant's Cerence Drive voice assistant system.

71. BIPA requires any private entity, such as Defendant, to obtain informed written consent from individuals before collecting or obtaining their biometric identifiers or biometric information. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through

trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

72. In each instance when Plaintiffs and the other Class members used their voice to interact with a voice assistant powered by Defendant's Cerence Drive biometric-enabled voice assistant system, Defendant captured, collected, or otherwise obtained Plaintiffs' and the other Class members' biometrics without their written consent and without complying with BIPA.

73. Defendant's practices with respect to capturing, collecting, storing, and using the biometrics of Plaintiffs and the Class members fails to comply with the following requirements of Section 15(b):

a. Defendant failed to inform Plaintiffs and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b. Defendant failed to inform Plaintiffs and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Defendant failed to inform Plaintiffs and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2); and

d. Defendant failed to obtain a written release, as required by 740 ILCS

14/15(b)(3).

74. As a result, Defendant has violated Section 15(b) of BIPA.

75. Defendant knew, or was reckless in not knowing, that integrating biometric-enabled voice assistant technology in automobiles sold and driven in Illinois and obtaining numerous Illinois residents' biometrics would be subject to Section 15(b) of BIPA, a statutory provision that was enacted in 2008.

76. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

77. Defendant's violations of Section 15(b) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(b) of BIPA.

78. Accordingly, with respect to Count I, Plaintiffs, individually and on behalf of the proposed Class, pray for the relief set forth below.

COUNT II
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d)
(On behalf of Plaintiffs and the Class)

79. Plaintiffs incorporate the foregoing allegations by reference as though fully set forth herein.

80. Defendant is a private entity subject to BIPA. 740 ILCS 14/10.

81. As discussed above, Defendant came into possession of Plaintiffs' and the other Class members' biometrics after they interacted with Defendant's Cerence Drive biometrically enable voice assistant technology.

82. Section 15(d) of BIPA prohibits any private entity in possession of biometrics, such

as Defendant, from disclosing, redisclosing, or otherwise disseminating an individual's biometric identifiers or biometric information without that individual's consent. 740 ILCS 14/15(d).

83. On information and belief, Defendant has disclosed or otherwise disseminated the biometrics of Plaintiffs and the Class members to third party companies. Specifically, Defendant's Cerence Drive platform utilizes user voice commands when connecting with and interfacing with third-party services such as cloud storage, external content services, and third-party assistants.

84. Defendant never obtained Plaintiffs' or other Class members' consent to disclose or disseminate their biometrics.

85. Accordingly, Defendant has violated Section 15(d) of BIPA.

86. Defendant knew, or was reckless in not knowing, that by utilizing a biometric-enabled voice recognition system that disclosed or disseminated the biometrics of numerous Illinois residents as alleged above, it would be subject to Section 15(d) of BIPA, a statutory provision enacted in 2008.

87. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

88. Defendant's violations of Section 15(d) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(d) of BIPA.

89. Accordingly, with respect to Count II, Plaintiffs, individually and on behalf of the proposed Class, pray for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, respectfully request that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiffs as class representatives, and appointing the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(2);

e. Awarding statutory damages of $1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(1);

f. Awarding reasonable attorneys' fees, costs, and other reimbursable litigation expenses pursuant to 740 ILCS 14/20(3);

g. Awarding pre- and post-judgment interest, as allowable by law; and

h. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiffs request a trial by jury of all claims that can be so tried.

Dated: June 17, 2024

Respectfully Submitted,

RANDOLPH FRESHOUR and VINCENZO ALLAN, each individually and on behalf of

similarly situated individuals

By: /s/ *Paul T. Geske*
One of Plaintiffs' Attorneys

Myles McGuire
Paul T. Geske
Colin Primo Buscarini
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
pgeske@mcgpc.com
cbuscarini@mcgpc.com

Attorneys for Plaintiffs and the putative Class

CERTIFICATE OF SERVICE

I, the undersigned, certify that on June 17, 2024 I filed the foregoing *Third Amended Class Action Complaint* with the Clerk of Court using the Court's CM/ECF system, which will cause a copy of said document to be electronically transmitted to all counsel of record.

By: /s/ *Paul T. Geske*
Paul T. Geske